Het kwetsbare Internet: penetratietests en veelvoorkomende zwakheden

R.L. Moonen

De bedreigingen van 'het Internet' zijn wijd en zijd bekend... hoewel niet inhoudelijk. Een middel om hiertegen op te treden, en om in staat te zijn vervolgens ook daadwerkelijk tegen de bedreigingen op te treden, is het uitvoeren van een penetratietest. Dat is een heuse poging tot inbraak – maar dan wel volgens het boekje. Wat er in dat boekje staat, wordt hier beschreven.

Inleiding

Hackers, en de bedreiging die zij vormen, zijn recentelijk veelvuldig het onderwerp van publicaties in mainstream media ([Klav98]). Naar aanleiding van een inbraak in computersystemen van een groot bedrijf of een overheid via Internet volgen vaak al snel sensationele berichten. Ook op Internet verschijnen artikelen op drukbezochte sites als www.antionline.com en www.net-security.org die zich vrijwel uitsluitend bezighouden met verslaglegging van inbraken in computersystemen via het Internet. Het is dus niet verwonderlijk dat bedrijven meer zekerheid wensen over de mate waarin zij zijn beveiligd tegen aanvallen vanaf Internet en welke zwakheden kunnen worden geïdentificeerd (en vermeden).

Eén van de manieren om meer zekerheid te krijgen is de Internet Penetratie Test (IPT). Een dergelijke test emuleert de activiteiten van een hacker om inzicht te krijgen in de beveiliging van de Internet-koppeling (meestal door middel van een firewall) en het achterliggende bedrijfsnetwerk. De toegevoegde waarde van een IPT bestaat eruit dat werkelijke verificatie plaatsvindt van de beveiligingsmaatregelen, in tegenstelling tot een audit of review waarbij wordt gekeken naar de technische configuratie en instellingen en de kwaliteit van het beheer van de koppeling. Tevens kan een IPT inzicht geven in de werking van de escalatiepaden, procedures en respons van de beheerorganisatie in het geval van een beveiligingsincident.

Het vinden van gaten in de beveiliging van een Internet-koppeling is een proces waarbij gebruik wordt gemaakt van diverse hulpprogramma's en informatiebronnen ([Duni99]). Maar waar wordt nu specifiek naar gezocht, en wat zijn de risico's van de vele bekende (en minder bekende) kwetsbaarheden in de beveiliging van Internet-koppelingen en de achterliggende systemen?

In dit artikel zal een overzicht worden gegeven van de werkzaamheden die dienen te worden uitgevoerd tijdens een penetratietest, en zullen enkele hulpmiddelen en veelvoorkomende kwetsbaarheden van Internet-gekoppelde systemen worden beschreven.

Penetratietests versus hacken

Een penetratietest wordt door velen gezien als een geautoriseerde 'hack'. Echter, een hack is geslaagd wanneer een beveiligingslek is gevonden, terwijl een IPT pas is geslaagd wanneer zoveel mogelijk beveiligingszwakheden zijn gevonden en een volledig gedocumenteerd verslag van de pogingen is geproduceerd, ongeacht of werkelijke penetratie van de koppeling of achterliggende systemen plaats heeft gevonden. De rapportage van de pogingen dient duidelijk weer te geven welke tests zijn uitgevoerd, welke zwakheden zijn aangetroffen, welk risico zij inhouden, en welke acties dienen te worden ondernomen om deze op te heffen. Een penetratietest omvat daarom veel meer dan alleen een 'geautoriseerde hack'.

Een ander verschil tussen een penetratietest en een hack is de informatie die vooraf bekend is aan de uitvoerder van de tests. Deze vooraf beschikbare informatie betreft netwerkadressen, namen van computersystemen (hostnamen) en eventueel telefoonnummers van inbelfaciliteiten en instellingen van netwerkcomponenten. Deze informatie kan niet alleen worden gebruikt ten behoeve van de eigenlijke penetratiepogingen, maar tevens kan op Internet worden gezocht naar deze informatie om zodoende te bepalen of zij publiekelijk beschikbaar is (hetgeen kan duiden op een informatielek[1]). Een hacker zal in het algemeen voldoende tijd hebben om deze informatie te verzamelen en zal daarin uiteindelijk meestal goed slagen ([Mein98]). Het vooraf beschikbaar hebben van bepaalde informatie tijdens een IPT is daarom tijdbesparend. In bijzondere gevallen kan het echter gewenst zijn in het geheel geen informatie vooraf beschikbaar te hebben om zodoende tevens te beoordelen of deze informatie op eenvoudige wijze is te verkrijgen voor een willekeurige hacker.

Deze verschillen maken dat de goede uitvoering van een penetratietest gebaat is bij een eenduidige procesmatige aanpak. Indien van tevoren vaststaat aan welke randvoorwaarden dient te worden voldaan, welke informatie van tevoren beschikbaar dient te zijn en welke werkzaamheden zullen worden uitgevoerd, kan een penetratietest efficiënt en effectief worden uitgevoerd, ondanks het feit dat verschillen tussen in gebruik zijnde Internet-koppelingen zeer groot zijn.

1) Het zoeken naar informatie door middel van search engines op Internet behelst op zijn beurt weer het gevaar van het bekend maken van sleutelwoorden als projectnamen, hostnamen en netwerkadressen. Om deze reden kan niet altijd klakkeloos worden gezocht op Internet, maar moet de tester een afweging maken tussen het risico van het bekend worden van deze informatie en het belang van het vinden ervan.

Het proces

Een IPT kan in drie hoofdfasen worden onderverdeeld, te weten:
* voorbereiding en planning;
* uitvoering;
* rapportage.

Voorbereiding en planning

Voordat met het uitvoeren van een IPT kan worden begonnen, dient tijdens de voorbereiding aan een aantal randvoorwaarden te worden voldaan. Deze randvoorwaarden omvatten minimaal de volgende elementen:
* ondertekening van een verklaring van vrijwaring;
* vaststellen van de reikwijdte (scope) van de tests;
* overdracht van informatie met betrekking tot de te testen componenten;
* beschikbaar krijgen of maken van testapparatuur;
* vaststellen van contactpersonen;
* inplannen van werkzaamheden.

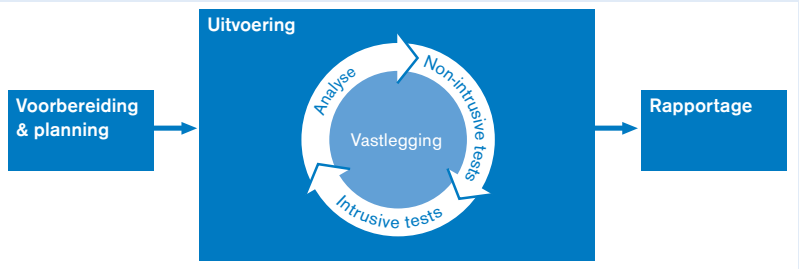
Met name het verkrijgen van een verklaring van vrijwaring en de vaststelling van de scope van de penetratietest zijn bij de voorbereidende fase van belang. De verklaring van vrijwaring dient de risico's van alle partijen te beperken in het geval onvoorziene beveiligingsincidenten of andere problemen optreden tijdens het testen. De scope dient verder accuraat te worden bepaald om te voorkomen dat onbedoeld componenten behorend tot derde partijen worden aangevallen (denk hierbij aan websites of routers die extern worden beheerd of gehost, maar wel binnen het domein van de te testen organisatie vallen).

Uitvoering

Na de voorbereidende fase kan met de uitvoering van de tests worden aangevangen. De uitvoering dient te allen tijde door een ervaren en op beveiligingsgebied terzakekundig persoon te gebeuren vanwege de risico's als het abusievelijk verstoren van productie, het beschadigen van bestanden, het abusievelijk hacken van componenten die niet behoren tot de doelomgeving en het onbedoeld lekken van confidentiële informatie door onzorgvuldigheid.

Tijdens de uitvoeringsfase wordt op verschillende manieren informatie verzameld, geanalyseerd en vastgelegd. Aan de hand van deze informatie wordt een poging ondernomen zwakheden en kwetsbaarheden te identificeren en zo mogelijk uit te buiten. Deze pogingen leveren in het algemeen nieuwe informatie op, die weer kan worden gebruikt voor verdere penetratiepogingen.

Figuur 1. Fasen tijdens een penetratietest.



Bij uitvoering kan onderscheid worden gemaakt tussen twee verschillende soorten tests: intrusive en non-intrusive tests. Intrusive tests zijn op daadwerkelijke penetratie gericht, terwijl non-intrusive tests erop gericht zijn informatie te vergaren die gebruikt kan worden voor verdere penetratie. Alle acties van zowel de intrusive als non-intrusive tests dienen te worden vastgelegd in een log ter latere verificatie en referentie in de rapportage.

Het vergaren van informatie via Internet (non-intrusive tests) via onder andere search engines, publiek toegankelijke databases en registratie-informatie vormt een belangrijk deel van deze fase, ondanks het feit dat deze niet is gericht op daadwerkelijke doorbreking van de beveiliging (omdat deze informatie de basis vormt voor de intrusive tests).

Rapportage

De rapportage van een penetratietest kan vele vormen aannemen, maar dient ten minste gedetailleerd verslag te doen van de volgende zaken:
* uitgevoerde werkzaamheden;
* geïdentificeerde zwakheden en kwetsbaarheden;
* aanduiding van het risico van de gevonden zwakheden en kwetsbaarheden;
* concrete aanbevelingen ten behoeve van opheffing van de zwakheden en kwetsbaarheden.

Voor de uitvoering van een IPT is de rapportagefase niet direct relevant. Wel dient ten behoeve van de rapportage een gedetailleerde log (vastlegging) aanwezig te zijn van alle acties en testresultaten die in het kader van de IPT zijn uitgevoerd.

Figuur 1 geeft een schematisch overzicht van de beschreven fasen weer.

Intrusive en non-intrusive tests

De hoofdmoot van de werkzaamheden van een IPT bestaat uit de intrusive en non-intrusive tests. Hieronder zal voor beide soorten tests worden ingegaan op de specifieke doelen en wijze van uitvoering van deze tests en de hulpmiddelen die daarbij kunnen worden gebruikt.

Non-intrusive tests

De non-intrusive tests pogen zoveel mogelijk informatie over de koppelingen en achterliggende systemen te vinden door het raadplegen van diverse publiek toegankelijke bronnen op Internet. Deze informatie is van belang, omdat pas kan worden aangevangen met de intrusive tests als voldoende achtergrondinformatie bekend is over de doelomgeving.

De benodigde informatie kan bijvoorbeeld bestaan uit namen van werknemers (wellicht worden deze namen gebruikt als wachtwoord), projectnamen, netwerkadressen van componenten of externe rapportages over de infrastructuur van de betreffende doelomgeving.

In tabel 1 is een overzicht gegeven van de soorten informatie die van belang kunnen zijn voor verdere tests, de

Type informatie	Bron	Zoeksleutel	Eventueel te vinden informatie
Geregistreerde Internet-domeinnamen, toegewezen Internet Protocol (IP)-adressen.	* www.demon.net/external/ntools.html * rs.internic.net * www.ripe.net	Bedrijfsnaam, geregistreerde handelsmerken.	Domeinnamen, technische en administratieve contactnamen, IP-adressen, e-mailadres van de postmaster.
Achtergrondinformatie over de eigenaar van de Internet-koppeling.	www.domein.naam	N.v.t.	Mogelijke projectnamen, afdelingsnamen, webmaster e-mailadressen, type en versie van de webserver-hardware en -software, e-commerce-applicaties beveiligingsinformatie, hardware- en softwareleveranciers, voornaamste leveranciers en klanten, namen van werknemers (mogelijk te gebruiken als gebruikersnaam of wachtwoord). Tevens: via de website aan te vragen brochures en persberichten.
Externe achtergrondinformatie over de eigenaar van de koppeling.	Search engines, zoals * www.metacrawler.com * www.hotbot.com * www.infoseek.com	Bedrijfsnaam, domeinnaam, IP-adressen, voornaamste leveranciers en klanten.	Relevante informatie. Mogelijk publicaties die bedrijfsnaam of klanten vermelden.
Usenet-artikelen komend van werknemers van het bedrijf.	www.dejanews.com	Domeinnaam, IP-adressen, contactnamen, namen van werknemers.	Relevante informatie. In technische discussiegroepen mogelijk detailinformatie over in gebruik zijnde hardware en software.
Documenten gerelateerd aan het bedrijf.	www.ftpsearch.com	Bedrijfsnaam of afkortingen en variaties daarvan.	Documenten of bestanden gerelateerd aan het bedrijf. Eventueel externe rapporten of onderzoeken.
Discussies in mailinglijsten over het bedrijf of van werknemers van bedrijf.	Search engines, zoals * www.metacrawler.com * www.hotbot.com * www.infoseek.com	Contactnamen van webmasters, systeembeheerders en andere technische staf, e-mailadressen.	Relevante informatie. In het bijzonder specifieke informatie over de doelomgeving, zoals infrastructuur, topologie van het netwerk, hardware en software.

Tabel 1. Overzicht informatie voor testen.

bronnen en eventueel welke zoeksleutels kunnen worden gebruikt ten behoeve van het doorzoeken van databases.

Intrusive tests en het uitbuiten van zwakheden

Intrusive tests zijn erop gericht daadwerkelijk toegang te krijgen tot de doelomgeving. Deze tests zijn om deze reden vaak agressiever van aard dan de non-intrusive tests en maken vaak gebruik van zwakheden in communicatieprotocollen en configuraties.

Communiceren via Internet wordt mogelijk gemaakt door een set communicatieprotocollen genaamd Transport Control Protocol/Internet Protocol (TCP/IP). Deze protocollen worden gebruikt om e-mail te versturen, bestanden op te halen en webpagina's te bekijken. Maar ook het vertalen van een hostnaam in een Internet Protocol-adres (IP-adres), het benaderen van fileservers en netwerkbeheer gebeurt door middel van TCP/IP.

Elke functionaliteit van Internet is geassocieerd met een protocol dat boven op het basiscommunicatieprotocol TCP/IP is gedefinieerd volgens het OSI-lagenmodel. Zo is het Simple Mail Transfer Protocol (SMTP) gedefinieerd om e-mail te kunnen verzenden en ontvangen, het File Transfer Protocol (FTP) om bestanden te kunnen versturen en het HyperText Transfer Protocol (HTTP) om webpagina's op te halen. Naast deze protocollen bestaan tientallen andere, soms obscure, protocollen ten behoeve van de vele functionaliteiten van het Internet.

De implementatie van al deze protocollen laat in veel gevallen echter te wensen over. Jaarlijks worden tientallen redelijk ernstige zwakheden gevonden in de protocollen en met name de implementaties en configuraties ervan. Vrij verkrijgbare, uitgekiende computerprogramma's (zogenaamde '*exploits*') kunnen deze zwakheden vaak effectief uitbuiten waardoor bedreigingen ontstaan als:

* het ongeautoriseerd verkrijgen van toegang tot systemen;
* het veranderen van informatie op systemen;
* het afluisteren van communicatie;
* het verhinderen van correcte werking van of communicatie met een systeem.

De aanwezigheid van zwakheden op systemen die gekoppeld zijn aan het Internet vormt een groot risico, omdat hackers geautomatiseerd kunnen zoeken (scannen) naar bekende zwakheden. Omdat ook de *exploits* om deze zwakheden uit te buiten vrij verkrijgbaar zijn op Internet is geen grote mate van specialistische kennis vereist om bekende beveiligingslekken te vinden en uit te buiten. Echter, een IPT dient niet alleen de meest bekende bedreigingen onder de loep te nemen, maar tevens minder bekende. Tevens mag nimmer op de correcte werking van deze exploits worden vertrouwd.

Het ideaal van een penetratietest is de vaststelling van de eventuele aanwezigheid van *alle* mogelijke zwakheden. Dit doel wordt in de meeste gevallen niet gehaald, omdat nooit kan worden vastgesteld dat alle mogelijke beveiligingslekken zijn gevonden. De bijlage 'Bedreigingen voor Internet-gekoppelde systemen' bevat een lijst met de meest voorkomende bedreigingen en zwakheden en het risico dat zij vormen ([Howa97]).

Commerciële hulpmiddelen voor het uitvoeren van intrusive tests

Bij de uitvoering van intrusive tests wordt vaak gebruikgemaakt van commercieel verkrijgbare security scanners. Deze software bezit een database van de meest voorkomende beveiligingslekken en poogt aan de hand van door de gebruiker opgegeven informatie de lekken in de beveiliging van de betreffende doelomgeving te identificeren.

Aan het gebruik van dergelijke tools zijn echter enkele beperkingen verbonden. Ten eerste pogen de meeste van deze scanners de gevonden gebreken niet, of slechts ten dele uit te buiten, waardoor een onvolledig beeld van de status van de beveiliging van de onderzochte componenten kan ontstaan. Tevens behoren de vaak meer sophisticated tests als tunneling (het verpakken van een protocol in het andere) en tests met gefragmenteerde TCP/IP-pakketten niet tot het repertoire van deze hulpmiddelen.

Ten tweede worden deze tools vaak als enig hulpmiddel gebruikt om penetratietests uit te voeren. Dit houdt in dat nieuw ontdekte lekken in implementaties en protocollen niet worden getest, omdat de databases van deze tools niet volledig up-to-date zijn.

Een derde beperking is de analyse van de resultaten. De meeste scanners pogen een classificatie van de risico's te verbinden aan de gevonden kwetsbaarheden. Het kan echter voorkomen dat enkele als 'low-risk' geclassificeerde kwetsbaarheden tezamen een reële bedreiging vormen voor de specifieke configuratie van de doelomgeving. Het blind varen op de uitkomsten van deze tools is daarom zeker niet aan te raden.

Deze beperkingen kunnen bij onoordeelkundig gebruik van een dergelijk product leiden tot een vals gevoel van veiligheid of juist een 'vals alarm'. Handmatige verificatie en analyse van de door deze hulpmiddelen geïdentificeerde kwetsbaarheden is daarom in alle gevallen noodzakelijk om een volledig beeld te kunnen vormen van de status van de beveiliging van de doelomgeving. Desalniettemin zijn commercieel verkrijgbare scanners een waardevol hulpmiddel bij het uitvoeren van penetratietests, omdat efficiënte uitvoering van een IPT gebaat is bij een snelle inventarisatie van mogelijke zwakke plekken.

Het periodiek scannen van een Internet-koppeling met behulp van een dergelijke scanner kan bovendien voor beheerders van de koppeling een uitstekende graadmeter zijn voor de huidige stand van de kwaliteit van de beveiliging[2]. Indien echter veel kwetsbaarheden worden geïdentificeerd is uitvoering van een volledige IPT altijd aan te raden.

Public domain hulpmiddelen

De hulpmiddelen die voor de verdere uitvoering van de intrusive tests van een IPT ter beschikking staan, zijn dezelfde als de hulpmiddelen die hackers ter beschikking staan. Deze via Internet vrij verkrijgbare programma's worden door de internationale gemeenschap van beveiligingsexperts ter beschikking gesteld met als doel systeembeheerders en beveiligingsconsultants dezelfde middelen in handen te geven als hackers. Helaas krijgen hiermee ook de wannabe-hackers en scriptkiddies[3] potentieel gevaarlijke tools in handen.

Deze tools bestaan vaak uit (een verzameling van) kleine programma's die specifiek een kwetsbaarheid pogen uit te buiten. *Exploits* zijn vaak alleen geschikt voor gebruik op Unix-platformen. De websites www.antionline.com en www.rootshell.com bevatten archieven van vrij te verkrijgen *exploits*.

Ook aan het gebruik van deze tools zijn beperkingen verbonden. De *exploits* die op deze plaatsen verkrijgbaar zijn, zijn vaak geschreven door onbekenden en zijn niet getest op correcte werking en integriteit[4]. Indien de *exploit* niet slaagt in het uitbuiten van de kwetsbaarheid, dan kan niet met zekerheid worden geconcludeerd dat geen risico bestaat.

Tot slot

Het beoordelen van de kwaliteit van de beveiliging van aan Internet gekoppelde systemen door middel van een IPT kan, mits uitgevoerd door terzakekundige professionals, additionele zekerheid leveren over de effectiviteit van de beveiligingsmaatregelen. Echter, door de zeer snelle veranderingen op dit gebied en de beperkte tijd waarin de IPT dient te worden uitgevoerd, kan nooit met volle overtuiging worden geconcludeerd dat een Internet-koppeling veilig is of dat de achterliggende systemen adequaat worden beschermd.

Indien na het uitvoeren van een audit of security review toch blijkt dat ongeautoriseerde toegang heeft plaatsgevonden via Internet, dan blijkt meestal dat veranderingen in de configuratie, nieuwe door een hacker of beveiligingsexpert ontdekte beveiligingslekken of menselijke fouten (het verliezen van wachtwoorden, het vergeten om modems uit te zetten) de bron van de penetratie zijn. Het is daarom, zeker bij de koppeling van productieve omgevingen aan het Internet, van belang periodiek verificatie te laten plaatsvinden van de kwaliteit van de beveiligingsmaatregelen. De IPT kan daarbij van grote waarde zijn.

Literatuur

[Duni99]
Tom Dunigan, *Tom Dunigan's Security Page, http://www.epm.ornl.gov/~dunigan/security.html*, Tom Dunigan, 1999.

[Howa97]
John D. Howard, *An Analysis Of Security Incidents On The Internet 1989-1995, http://www.cert.org/research/JHThesis/Start.html*, CERT/CMU, 1997.

[Klav98]
Marie-Jose Klaver, *Hacken tussen creativiteit en criminaliteit, http://www.xs4all.nl/~mjk/artikelen/hacken.html*, NRC Handelsblad, 31 december 1998.

[Mein98]
Carolyn P. Meinel, *Computer Security and the Internet*, Scientific American, October 1998.

2) Het nut van het scannen van standaard-firewalloplossingen met deze scanners is echter beperkt. Bouwers van firewalls en andere beveiligingsproducten zorgen er in het algemeen voor dat hun producten van tevoren met deze scanners zijn getest en geen serieuze bevindingen veroorzaken.
3) Wannabe's en scriptkiddies zijn onervaren, beginnende hackers die slechts in staat zijn van Internet gehaalde scripts en exploits te draaien, vaak zonder te weten wat exact wordt uitgebuit en zonder zich van de gevolgen bewust te zijn.
4) Op Internet zijn bijvoorbeeld BackOrifice-verwijderaars aangetroffen en aangeprezen die BackOrifice juist installeren terwijl zij melden het te hebben verwijderd.

Bijlage: Bedreigingen voor Internet-gekoppelde systemen

Scans

Door handig gebruik te maken van diverse bestaande netwerkprotocollen van de TCP/IP-set kunnen scans worden uitgevoerd op netwerkdelen of individuele computers. Scans hebben tot doel te inventariseren welke hosts op een netwerkdeel welke diensten actief hebben. Ook kan door middel van een scan vaak worden vastgesteld welk besturingssysteem een computer of component bezit, omdat vrijwel alle componenten op verschillende wijze reageren op bepaalde scans. Deze informatie is van belang om potentiële kwetsbaarheden te identificeren.

Pingscan en poortscan

Een zogenaamde pingscan stuurt een verzoek tot antwoord naar elk IP-adres in een opgegeven lijst of reeks. Uit de antwoorden kan worden opgemaakt op welke IP-adressen zich computers bevinden die benaderbaar zijn. Een 'ping' wordt normaal gesproken gebruikt om verbindingen te testen en responstijden te meten. Hoewel een pingscan geen directe bedreiging vormt voor de beveiliging van een Internet-koppeling of de achterliggende netwerken, kan het gewenst zijn de informatie die een pingscan levert niet beschikbaar te laten zijn vanaf het Internet, omdat hiermee aanvallen eenvoudiger en efficiënter kunnen worden uitgevoerd.

Een poortscan is een scan die de beschikbare netwerkdiensten in kaart brengt. Aan de hand van de TCP/IP-poorten die beschikbaar zijn, kan worden vastgesteld welke diensten een host aanbiedt omdat de meeste diensten zijn geassocieerd met een vaste poort. Zo wordt ten behoeve van het HTTP-protocol poort nummer 80 gebruikt, ten behoeve van SMTP poort nummer 25 en voor de Domain Name Server (DNS) poort nummer 53.

Voor het uitvoeren van poortscans en pingscans zijn diverse hulpmiddelen publiekelijk beschikbaar, zoals 'nmap', 'netcat' en 'ping-it'.

Denial of Service

Denial of Service (DoS) attacks zijn de nieuwe plaag voor systeembeheerders en Internet Service Providers. DoS-aanvallen worden ook wel 'nukes' genoemd en zijn in de meeste gevallen getooid met fantasierijke namen als 'smurf', 'teardrop', 'land', 'bonk', 'snork' en 'WinNuke'. Dit type aanvallen tracht meestal door misvormde of bijzondere datapakketten de ontvangende computer tot afwijkend gedrag te dwingen. Aangezien de communicatie hierbij vaak maar één kant op gaat (van aanvaller naar slachtoffer) kan het TCP/IP-afzendadres van een dergelijk datapakket eenvoudig worden vervalst. Hierdoor is het vaak onmogelijk de dader van een DoS-aanval te achterhalen.

Sommige DoS-aanvallen kunnen een netwerk binnen enkele seconden onbruikbaar maken door een sneeuwbaleffect teweeg te brengen. Incidenten van dit soort DoS-aanvallen nemen de laatste tijd zeer sterk in aantal toe. Bescherming tegen DoS-aanvallen is echter een moeizame kwestie, daar leveranciers meldingen van deze kwetsbaarheden pas sinds kort serieus nemen. Hierdoor zijn veelgebruikte operatingsystemen als Windows NT en diverse 'smaken' Unix in het bijzonder kwetsbaar voor deze aanvallen.

Vanwege de relatieve eenvoud van de aanvallen, de vrije beschikbaarheid van de programmatuur om ze uit te voeren en de mogelijkheid als aanvaller anoniem te blijven, valt te verwachten dat deze vorm van vandalisme een grote bedreiging gaat vormen voor productieomgevingen die zijn gekoppeld aan het Internet.

Trojans

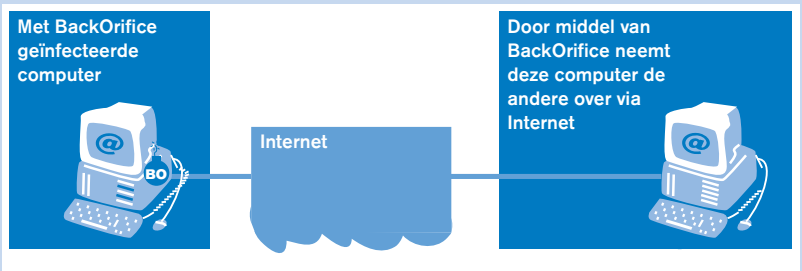
Trojans is de verzamelnaam voor programma's die zich verstoppen in systemen of zich voordoen als legitieme software, terwijl ze in werkelijkheid informatie over de gebruiker of het systeem doorgeven aan de aanvaller. Hoewel trojans strikt genomen geen zwakheid van Internet-koppelingen inhouden en tot voor kort relatief weinig voorkwamen, is met de komst van BackOrifice en NetBus toch een bedreiging voor Internet-koppelingen ontstaan.

BackOrifice en NetBus zijn client-serverapplicaties om op afstand een PC met Windows 95, 98 of NT te besturen via het Internet (of een Local Area Network (LAN) met TCP/IP-functionaliteit). Deze functionaliteit bestaat al veel langer; onder andere PCAnywhere en RemotelyPossible bieden deze functionaliteit via inbelfaciliteiten. Het grote verschil tussen deze programma's en BackOrifice en NetBus is dat laatstgenoemde via Internet opereren en zichzelf 'verstoppen' en dus onzichtbaar blijven voor de gebruiker van een met BackOrifice (of NetBus) geïnfecteerde computer. Slechts een gerichte zoekopdracht in specifieke bestanden of een recente virusscanner op een computer zal de aanwezigheid van deze trojans prijsgeven.

Deze trojans kunnen, indien op een PC geïnstalleerd, worden gebruikt om dataverkeer op een netwerk af te luisteren, bestanden te kopiëren of wachtwoorden te stelen. Het installeren van BackOrifice of NetBus dient wel door de gebruiker zelf te gebeuren, maar kan worden verstopt in de installatieprocedure van legitieme software. Hierdoor kunnen BackOrifice en NetBus worden geclassificeerd als een trojan.

De bedreiging die programma's als BackOrifice en NetBus vormen kan momenteel moeilijk worden ingeschat, maar de verwachting is dat deze nieuwe trojans en andere zwakheden die het mogelijk maken ongezien dergelijke programma's te installeren, een zeer risicovolle

Figuur 1. Het gebruik van BackOrifice.



combinatie zullen vormen. Het gericht zoeken naar BackOrifice en aanverwante kwaadaardige programmatuur op Internet-koppelingen en achterliggende systemen is daarom een integraal onderdeel van een IPT.

Buffer overflows

Netwerkdiensten als e-mail, ftp en WWW maken alle gebruik van eigen protocollen. Naast de zwakheden die deze protocollen inherent kunnen hebben, is de implementatie ervan vaak een bron van kwetsbaarheden. Een bijzonder vaak voorkomende vorm van die zwakheden is de zogenaamde buffer overflow.

Een buffer is een klein stukje toegewezen geheugen waarin tijdelijk een wachtwoord, gebruikersnaam of commando wordt opgeslagen. Een veelvoorkomende (en eenvoudig te voorkomen) programmeerfout zorgt ervoor dat niet wordt gecontroleerd of de aangeboden data daadwerkelijk in het stukje geheugen passen. Indien deze controle ontbreekt is het vaak mogelijk zodanig het geheugen te manipuleren door het aanbieden van te grote hoeveelheden data dat zelfgekozen kwaadaardige programmacode wordt uitgevoerd (zie figuur 2). Deze instructies zouden kunnen bestaan uit het verlenen van ongeautoriseerde toegang tot het systeem of het installeren van BackOrifice.

Buffer overflows vormen momenteel de grootste bedreiging voor de beveiliging van computers die aan Internet zijn gekoppeld, omdat veel leveranciers systemen en software leveren die in hun standaardconfiguratie kwetsbaar zijn voor dit type aanval. Veel leveranciers verzuimen echter klanten tijdig op de hoogte te stellen van deze kwetsbaarheden. In het afgelopen jaar zijn ten minste veertig van dergelijke kwetsbaarheden in commerciële besturingssystemen en software (waaronder browsers en e-mailclients) ontdekt.

Spoofing

Spoofing (in deze context) is de algemene benaming voor het zich voordoen als iets of iemand anders. Het vervalsen van het e-mailafzendadres is een vorm van spoofing, evenals het overnemen van bestaande verbindingen ('hi-jacking') of het vervalsen van Domain Name System (DNS)-informatie. Spoofing is vaak mogelijk door het gebruik van ondoordachte protocollen, of fouten in de implementatie ervan.

TCP/IP-spoofing is bijzonder vanwege een aantal redenen. Ten eerste betreft TCP/IP-spoofing meestal het ongeautoriseerd wijzigen van gegevensstromen, in tegenstelling tot het binnendringen in een computersysteem of vervalsen van een e-mailadres. Indien de gegevensstromen van een netwerkdeel kunnen worden beïnvloed, dan kan de impact van spoofing zeer groot zijn. Ten tweede is spoofing vaak bijzonder lastig uit te voeren vanwege timingproblemen en wiskundige analyses die moeten worden uitgevoerd om succesvol te zijn. Dit maakt het opsporen van potentiële kwetsbaarheden met betrekking tot TCP/IP-spoofing een lastig probleem.

CGI-hacks

Alle verkrijgbare webserver-software bevat een standaardkoppelvlak naar programmatuur die kan worden gebruikt om bijvoorbeeld databases te raadplegen op websites, spelletjes te spelen via de homepage of aanvragen te doen voor informatie. Deze standaard, Common Gateway Interface (CGI), stuurt op onbeveiligde wijze informatie door naar de achterliggende programmatuur (bijvoorbeeld database-applicaties, spelletjes, e-mailsoftware).

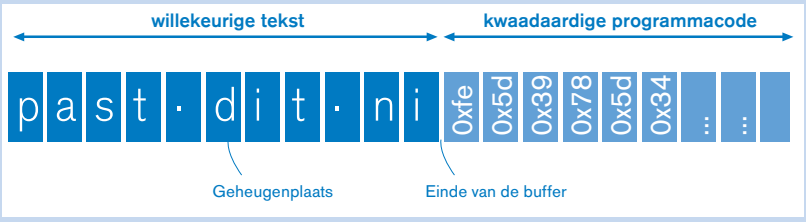
Het is de verantwoordelijkheid van deze achterliggende programmatuur (vaak snel en slordig ontwikkelde scripts) om de informatie die wordt doorgestuurd te controleren op integriteit en juistheid. Het komt echter bijzonder vaak voor dat deze controle niet wordt uitgevoerd of onvolledig is, waardoor het mogelijk wordt de achterliggende scripts zodanig te manipuleren dat willekeurige taken kunnen worden uitgevoerd, zoals het aanpassen van homepages of het verlenen van ongeautoriseerde toegang tot websites. Naar schatting zijn CGI-hacks verantwoordelijk voor negentig procent van de gevallen waarbij homepages van grote instellingen en bedrijven zijn veranderd.

Configuratiefouten

Buiten de hierboven beschreven zwakheden en gevaren bestaat een groot deel van de kwetsbaarheden van Internet-gekoppelde systemen uit foutief geconfigureerde netwerkcomponenten. Zo kan een verkeerd ingestelde toegangscontrolelijst (access list) op een router onbedoeld toegang geven tot het interne bedrijfsnetwerk. Vaak is de configuratie van firewalls dermate complex dat foutjes ontstaan in de filtering van verkeer of kan een verkeerd geconfigureerde DNS plotseling informatie bevatten over interne systemen die niet bekend had mogen worden buiten de Internet-koppeling.
Deze fouten zijn moeilijk te voorkomen, maar kunnen door middel van periodieke controle en verificatie wel worden gevonden.

Backdoors

In sommige actieve netwerkcomponenten of computers hebben fabrikanten achterdeuren ingebouwd. Dit zijn meestal ongedocumenteerde wachtwoorden die toegang tot de component verschaffen. Vaak zijn deze achterdeuren bekend bij hackers en vormen zij derhalve een grote bedreiging voor de beveiliging van deze componenten. Het is meestal niet mogelijk de achterdeuren te verwijderen, doordat zij door de fabrikant worden meegeleverd met de hardware. Gelukkig komen backdoors steeds minder voor, hoewel de meeste populaire BIOS'sen van PC's en sommige populaire netwerkswitches nog steeds backdoors bevatten.



Figuur 2.
Buffer overflow.